pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Virtual Private Network Standards

ITP Number ITP-SEC010	***Effective Date*** 3/17/2014
Category Recommended Policy	***Supersedes*** None
Contact RA-ITCentral@pa.gov	***Scheduled Review*** As needed basis

This Information Technology Policy (ITP) establishes policy, standards, and procedures associated with the use of Virtual Private Networks (VPNs).

1. Purpose

This Information Technology Policy (ITP) provides guidance and standards to commonwealth agencies to mitigate the risks associated with the transmission of sensitive information across networks by implementing Virtual Private Networks (VPNs) based on Internet Protocol Security (IPSEC) and the Secure Sockets Layer (SSL) protocol.

2. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

The requirements in this policy are the minimum adequate to provide an acceptable level of encryption

3. Objective

IPSEC, which is defined by the Internet Engineering Task Force, consists of a set of open standards to provide security equivalent to a private network in the shared infrastructure (Internet). IPSEC provides security at the network layer, and also provides security to all the packets of applications belonging to a security policy.

IPSEC is designed to provide interoperable, high-quality, cryptographically based security for VPNs. The set of security services offered includes access control, connectionless integrity, data origin authentication, replay protection (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality.

SSL VPNs use a different methodology to transport data confidentially over a public network. In contrast to the traditional IPSEC VPN, SSL VPNs use a secure transport mechanism that is built-in to all standard Web browsers. SSL, which is implemented in the application layer, secures the HTTP protocol and it offers encryption, source authentication, and data integrity as a means to protect information exchanged over insecure, public networks.

4. Policy

This ITP represents the minimum operational standards for network-based IPSEC VPN and SSL VPN between trusted and untrustworthy networks. The following are two VPN integrated models that allow an agency to securely connect remote users and systems:

Gateway-to-Gateway VPN minimum policy requirements

This model protects communications between two specific networks, such as from one agency central office network to another, from an agency central office network to another internal agency branch office network, or between an agency's central offices to trusted business partners.

Host-to-Gateway VPN minimum policy requirements

This model protects communications between one or more individual hosts and a specific network belonging to an agency. The host-to-gateway model is most often used to allow hosts on unsecured networks, such as traveling employees and telecommuters, to gain access to internal organizational services. Split-tunneling (which allows a VPN user to access a public network (e.g., the Internet) and a second VPN connection or WAN at the same time, using the same or multiple physical network connections) is prohibited. LAN Access to local resources (printers, file shares) while connected to VPN is permitted.

Two-factor authentication as described in ITP-SEC014 – *Identity Protection and Access Management (IPAM) Architectural Standard - (Product Standards for Public Key Infrastructure/Shared Service Provider),* is to be utilized for a Host-to- Gateway VPN.

Agencies are to comply with product standards as described in this document *and* ITP-SEC031 - *Encryption Standards for Data in Transit.*

VPN Two-Factor security token requirements

Two-Factor Authentication requires users to provide two proofs of their identity, which increases security for access to commonwealth resources. It reduces the risk that business or personal information stored in administrative systems will be compromised. The type of two factor authentication mechanism required for remote access shall be dependent upon the sensitivity level of the resources being accessed or the privilege level of the user role accessing resources. The following chart below identifies the minimum two factor authentication methods required for remote access to commonwealth resources.

Enterprise Systems	Access Method	Security Token / Digital certificate authentication
Current Telecom Service Provider Systems	Verizon's (ISIS) management console	Minimum requirement – Security Token
Commonwealth Systems	Remote VPN connection	Minimum requirement – Digital Certificate

Enterprise Roles	Access Method	Security Token / Digital certificate authentication
Enterprise CWOPA Active Directory administrators	Remote VPN connection	Minimum requirement – Security Token

VPN Network Access Control endpoint checks:
VPN elements of an end point check will be enforced to check for current Anti- Virus software, and Operating System security patches before the remote user will be allowed access to the network.

The following are requirements related to all agency managed or enterprise remote access systems, subject to change:

Operating System:
Broadband Connection List of supported Operating Systems:

https://itcentral.pa.gov/Documents/j-sa-sslvpn-7_4r7-supportedplatforms.pdf

List of supported Operating Systems for Dial Up Access:

Windows Vista	32/64 bit
Windows 7	32/64 bit
Windows 8/8.1	32/64 bit

Anti-Virus and Security Patches:
List of supported Anti-Virus packages here:
http://www.juniper.net/support/products/esap/

- Anti-Virus definitions need to be in compliance within a maximum of 10 definition file versions from the vendor's latest release.

- Full System scan (memory, drives, registry, and running processes) performed within the past 30 days.

- Operating System security patches need to be in compliance within a maximum of 30 days from the latest vendor's release date.

5. Standards

Enterprise Product Standards

(These technologies meet the requirements of the current architecture and are recommended for use.)

Technology	Platforms	Category	Technology Classification
Current Telecom Service/Product Offerings	Current Telecom Service/Product Offerings	VPN	Current

CONTAIN

(These technologies no longer meet the requirements of the current architecture and are not recommended for use. They are to be phased out over time. No date has been set for their discontinuance.)

Technology	Platforms	Category	Technology Classification
Check Point VPN Security Suite	Checkpoint VPN-1 Checkpoint Connectra	VPN	Contain
Cisco Systems Integrated Switch/Router	Cisco IOS IPsec VPN Cisco IOS SSL VPN	VPN	Contain
Security	Cisco Catalyst 6500 Series/7600 Series WebVPN Services Module Cisco 7600 Series/Catalyst 6500 Series IPSec VPN Shared Port Adapter		Contain
Cisco Systems VPN Appliances	Cisco ASA 5500 Series Adaptive Security Appliances Cisco PIX 500 Series Security Appliances Cisco VPN 3000 Series Concentrators	VPN	Contain

RETIRE

(These technologies are being phased out. Plans are to be developed for their replacement, especially if there is risk involved, such as lack of vendor support. A date for retirement has been set.)

Technology	Platforms	Category	Technology Classification
--	--	--	Retire by mm/dd/yy

EMERGING / RESEARCH

(Emerging technologies have the potential to become current standards. At the present time, they are to be used only in pilot or test environments where they can be evaluated. Use of these technologies is restricted to a limited production mode, and requires approval of a waiver request.

Research technologies are less widely accepted and time will determine if they will become a standard.)

Technology	Platforms	Category	Technology Classification
--	--	--	Emerging / Research

6. Related ITBs/Other References

- ITP-PLT012 – *Use of Privately Owned PCs to Access CoPA Resources*
- ITP-SEC014 – *Identity Protection and Access Management (IPAM) Architectural Standard - (Product Standards for Public Key Infrastructure/Shared Service Provider)*
- ITP-SEC031 – *Encryption Standards for Data in Transit*

7. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

8. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	6/22/06	Base Document
Revision	8/1/12	Align to the changes in security under the current telecommunications contract. Differentiate between supported operating systems for Dial-Up connections and Broadband connections. Added grace period for host-checks. Clarified split- tunneling definition. Modified DAT file definition.

Revision	12/05/12	Incorporated STD-SEC010A - Product Standards for Virtual Private Networks and clarifying language concerning two-factor authentication methods.
Revision	12/05/13	ITP Refresh – converted ITB to ITP format
Revision	3/17/14	Removed Windows XP from supported list of operating systems. Added Windows 8/8.1 to supported list of operating systems.